REMARKS

Claims 9-26 and 30 are pending in the patent application. The Examiner has rejected Claims 9-26 and 30 under 35 USC 112; has rejected Claims 9-18, 21-22, 25-26 and 30 under 35 USC 103 as unpatentable over the combined teachings of Merritt, Manduley and Hoss; Claim 19 under 35 USC 103 as unpatentable over the combined teachings of Merritt, Manduley and Hoss further in view of Abraham; Claim 20 under 35 USC 103 as unpatentable over the combined teachings of Merritt, Manduley and Hoss further in view of Lessin; and Claims 25 and 26 under 35 USC 103 as unpatentable over the combined teachings of Merritt, Manduley and Hoss and further in view of Schneier. For the reasons set forth below, Applicants respectfully assert that the claims, as amended, are patentable over the cited art.

The present invention teaches and claims a device, terminal, server, program storage device, and method for establishing trustworthy connections among a user, with or without a device inserted at a terminal, a terminal, and a server. Specifically, the user must know that the terminal is trusted by the server before the user will release any sensitive information to the terminal. Similarly, the

server must know that the terminal seeking access to it is authentic. The server may also engage in an exchange to determine if the user, of a user device or of the terminal, is authorized to access the server. In all claimed embodiments of the invention, the server authenticates the terminal. Once the terminal has been authenticated, the server communicates that information along the second connection between the user device and the server, without communicating that information along the connection between the server and the terminal. The server either communicates that information directly to the user by display at the user device, or communicates that information to the user by notifying the user device whereupon the user device causes the terminal to display the information to the user, when the user has a device that does not have display capabilities. Applicants respectfully assert that none of the cited prior art teaches or suggests a server communicating terminal authentication information directly to the user device along a connection between the server and the user device. Applicants also assert that none of the prior art teaches or suggests that terminal authentication information be communicated to the user, whereupon the user or user device provides information to the terminal for the

terminal to dynamically create a user-specific authenticity output message for display to the user. None of the cited art teaches or suggests that a terminal dynamically create an authenticity output message.

The Examiner has noted that the claims do not recite dynamically creating the authenticity output message, do not recite a user-specific authentication message, and do not recite communicating the terminal authentication message directly. While Applicants believe that the claims were clear, the claims have been amended to address the Examiner's remarks.

The primary reference cited against the present application is the Merritt patent. The Merritt patent teaches a method for authenticating a terminal whereby a terminal contacts the server, followed by the server and the terminal engaging in an authentication process, referred to as a "two-way challenge-response" (Col. 4, lines 57-64). Once the server and the terminal have mutually authenticated themselves to each other, the terminal sends the user's account information to the server, the server retrieves a user-specific personal security phrase ("PSP") from its storage, and the server sends the PSP to the terminal. The terminal displays the PSP to the user, prompting the user to verify

that the PSP is correct, preferably by user entry of a personal identification number (PIN) (see: Col. 6, lines 21-36). Under the Merritt method, the server does not generate an authenticity output message and does not communicate a generated authenticity output message to the user along a connection which is separate from the connection between the host and the terminal. Rather, under the Merritt system, the server authenticates itself and sends that information to the terminal while the terminal authenticates itself and sends that information to the server. The Merritt server does not authenticate the terminal, but authenticates *itself* (i.e., the server) to the terminal (Col. 4, lines 60-64). The server does not authenticate the terminal and does not generate any authenticity output message regarding the authenticity of the terminal. Further, under Merritt, the user does not receive any authentication information, from either the terminal or the server. The user simply gets prompted with his PSP. The user does not have a separate connection with the host and does not receive terminal authentication information from the host.

With specific reference to the language of independent Claim 9, Applicants respectfully assert that the Merritt patent does not teach or suggest the invention as claimed.

The Merritt system does not teach or suggest that the server has a communication component for establishing and conducting communications with a terminal along a first trusted connection and for establishing and conducting communications with a user along a second trusted connection. Merritt provides one communication line, 9 of Fig. 1, between the host/server and the terminal. Merritt does not teach or suggest that the user have a separate connection with the server. Applicants contend that communicating along the one connection, 9 of Fig. 1, between the host/server and the terminal does not teach or suggest a second trusted connection between the server and the user, which second trusted connection is separate from the first trusted connection between the server and the terminal. In response to the 112 rejection of this language, Applicants aver that throughout the Specification, the authenticated trusted connections are clearly indicated as separate (see: S-T and S-D on page 9, step 3 through page 10, step 5; c1 and c2 at page 12, lines 3-9; c1 and c2 on page 13, lines 14-18; and S-T and S-D on pages 16-17, etc.). Applicants contend that the Specification is clearly teaching separate connections, as would be clear to one having skill in the

relevant art from a reading of the teachings referenced above.

The claim language of Claim 9 also expressly recites that the server has at least one authentication component for verifying the authenticity of the terminal. According to the teachings found in Merritt at Col. 4, lines 60-64, however, the server authenticates *itself* to the ATM terminal (in step 340 of Fig. 3) but does not authenticate the terminal, per se. While Fig. 1 of Merritt does illustrate a comparator component and RN generator, Merritt does not teach that the components comprise an authentication component for verifying the authenticity of a terminal. The Examiner additionally cites Fig. 3, element 315 against the authenticity component. What is illustrated at 315 of Fig. 3 is the process step of the two-way challenge-response process. Element 315 does not illustrate a server authentication component. Finally, the Examiner cites the passage found from Col. 2, lines 10-14 against the claimed at least one authentication component. The cited passage states that there is a need to authenticate a terminal to a user. Neither the cited passage nor the ensuing Merritt teachings, however, expressly teach that the terminal is authenticated by the server.

The independent Claim 9 further recites a message generation component for generating at least one authenticity output message for delivery to the user along the second trusted connection. Applicants first assert that Merritt does not teach or suggest that its host server has a message generation component or that the server generates an authenticity output message. The Examiner cites element 3 of Fig. 1 as showing both a message generation component and a storage location (see: the top of page 9 of the Office Action). What Fig. 1, element 3 illustrates is a database. The only teachings of the host accessing that database are found at Col. 6, lines 22-23 and at Col. 7, lines 5-7 where the host retrieves the PSP and account information from the database. Applicants argue that it is clear that the Merritt element 3 database is not a message generation component but is simply a storage location. The Examiner also appears to analogize retrieving and displaying the PSP to the dynamic generation and display of an authenticity output message indicating that the terminal has been authenticated. Applicants assert that Merritt does not teach or suggest that the PSP is a terminal authenticity message. The PSP is a retrieved user identifier. Applicants further reiterate that the PSP is delivered from

the host to the terminal along the one connection. The PSP is not a terminal authenticity message which is send to the user along a second trusted connection, separate from the connection between the server and the terminal. There is no teaching or suggestion in Merritt of a second trusted connection between the host and the user, separate from the connection between the host and the terminal, along which an authenticity message could be communicated.

Applicants maintain that the Merritt patent does not teach or suggest the steps of establishing a first authenticated trusted connection upon authenticating the terminal and of establishing a second trusted connection between the server and the user device upon authenticating itself to the device, wherein the first trusted connection is separate from the second trusted connection, as is expressly recited in the independent claims. Merritt does not teach or suggest separate connections. Applicants further assert that Merritt does not teach or suggest any communications between the host and the user that do not involve the ATM terminal. The Examiner, on page 3 of the Office Action, cites reference numeral 380 against the second trusted connection. However, reference numeral 380 illustrates the step of "ATM Communicates PSP to Customer".

Clearly the ATM displaying the PSP to the user is not the same as or suggestive of the server communicating a terminal authenticity output message to the user along a second trusted connection, and not communicating that message along the connection between the server and the terminal. Rather, the Merritt ATM is displaying information which was received by the terminal from the host along the only connection.

Applicants further assert that the additionally cited Manduley patent does not provide the teachings which are missing from the Merritt patent. The Examiner acknowledges that the Merritt patent does not teach or suggest providing a terminal authenticity message to the device. The Manduley patent teaches a method for assuring that the user is actually in possession of the card. The invention as set forth in independent claim 12 expressly recites the server providing a terminal authenticity message to the device via the established second trusted connection. As claimed, the user device is being provided with confirmation that the terminal has been authenticated. User authentication is not being claimed. Moreover, sending terminal authentication information directly from a server to a user device along a connection which is separate from the connection between the terminal and the server, thereby eliminating the possibility

of a terminal interfering with or falsely generating a terminal authentication message, is not taught or suggested by the Manduley device display. Neither Manduley nor Merritt teaches that a terminal authentication message be communicated directly to the user device along a separate connection between the user device and the server, without also communicating the message along the connection between the terminal and the server. Since that limitation is not taught or suggested by the cited references, and since that limitation is recited in all of the remaining pending claims, it cannot be concluded that the claims are rendered obvious by the combination of teachings of Merritt and Manduley.

The Examiner has stated that Manduley teaches that the "smartcard contains an LCD display that will, at the request of the server/issuing authority, display a message to the user", citing Col. 3, lines 11-16 and lines 47-58. However, displaying at the device/card is not sufficient to render the claims unpatentable. Even if one were to modify Merritt so that the user device could display the PSP, rather than the terminal displaying the PSP, one would not arrive at the invention as claimed.

The Examiner has newly cited the Hoss patent for its teachings related to sending a message along a first trusted connection between a terminal and a server. Applicants respectfully maintain that none of the cited patents teaches or suggests two different connections. None of the patents teaches or suggests providing a terminal authenticity message, and none teaches providing that message via an established second connection between the user device and the terminal without also communicating that message to the terminal along the first connection. Since none of the references teaches the claim features, a *prima facie* case of obviousness simply has not been presented by the Examiner *(In re Wilson,* 424 F.2d 1382, 165 USPQ 494 (C.C.P.A. 1970)). The addition of the teachings of the Schneier reference to the combination of Merritt and Manduley do not render the invention obvious. While Schneier can output a number to represent a message, there is nothing in Schneier which would lead one having skill in the art to modify the combination of Merritt and Manduley to include communication of terminal authentication along a connection between a server and a user device and not along a different connection between the terminal and the server.

The addition of the Lessin patent teachings to the combination of Merritt and Manduley does not render the pending claims obvious. Lessin has been cited for teaching that a user enter a PIN. The combination of Merritt, Manduley and Lessin would again effectively teach away from the claimed invention since the user would be forced to enter his PIN at a terminal before establishing that the terminal was trusted. Clearly that does not obviate the language of Claim 20, which expressly states that the server first send terminal authentication information directly to the user device and not the terminal for authenticating the user.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,
N. Asokan, et al

By: Anne Vachon Dougherty
Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910